

REMARKS

The above-identified application is United States application serial number 10/037,593 filed on October 19, 2001. Claims 1-53 are pending in the application. Claims 1-53 are rejected.

Rejection of Claims Under 35 USC § 102

Claims 1-53 are rejected under 35 U.S.C. 102(e) as being anticipated by Khan et al. U.S. Patent Publication No. 2002/0116508A1 (hereinafter "Khan"). Applicant respectfully traverses these rejections.

Claim 1 has been amended to include the features of Claim 4 (now canceled), and recites:

A system for controlling transmission of data packets through an information network, comprising:

a Regional Transaction Processor (RTP); and

a Data Enabling Device (DED) operable to:

receive one or more data packets from the information network,
detect when the one or more data packets include content match
information, and

issue a message to a workstation and invoke the RTP to process a
transaction when the content match information is detected in
the one or more data packets, wherein the DED is operable to
prevent further transmission of the one or more data packets
based on the content match information.

Khan does not detect when the data packets include content match information and prevent further transmission of the one or more data packets based on the content match information. In contrast, Khan detects content match information in a first data packet containing the biometric information, and then determines whether to prevent transmission of different data packet(s) containing a message from the user. (Khan, paragraphs [0053], [0055], and [0061]). Claim 1 is distinguishable from Khan for at least these reasons.

KOESTNER BERTANI LLP
18562 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0250

Claims 2, 3, and 5 - 17 depend from Claim 1 and include features that further distinguish them from the prior art. For example, Claim 3 recites "the DED is operable to detect when the one or more data packets include content match information at a rate proportional to the rate at which the data packets are received." In contrast, the cited portions of Khan disclose using different types of biometrics, including the biometric on the envelope, and authenticating the sender's digital signature. (Khan, paragraphs [0060] and [0067]). Khan does not disclose or suggest detecting when the one or more data packets include content match information at a rate proportional to the rate at which the data packets are received.

As another example of distinguishing features in the claims, Claim 11 recites "the DED includes Field Programmable Gate Arrays (FPGAs)." In contrast, the cited portions of Khan disclose use of a virtual envelope that is created by a software application, and authenticating the biometric of the sender. (Khan, paragraph [0059]).

Further, Claim 13 recites "a portion of the DED can be dynamically reprogrammed and the DED is operable to continue processing the data packets during the partial reprogramming." The cited portion of Khan does not disclose or suggest such a feature, but rather teaches integrating biometric identity technologies, and using a public key/private key to encrypt/decrypt the message. Nothing in Khan discloses or suggests reprogramming the DED or that the DED continues processing data packets during the reprogramming.

Independent Claim 18 has been amended to include the features of Claim 20 (now canceled), and recites:

"A method for controlling transmission of identifiable content over an information network, comprising:

- providing content match information for the content to a DED, wherein the DED is located in the information network along a transmission path of a plurality of data packets, wherein at least one data packet includes the content match information;
- receiving the at least one data packet in the DED;
- detecting the content match information in the at least one data packet in the DED;

KOESTNER_BERTANI_LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL: (949) 251-0250
FAX (949) 251-0260

issuing a prompt to a workstation based on the content match information when the content match information is detected in the at least one data packet; and
preventing further transmission of the one or more data packets based on the content match information."

Khan does not detect when the data packets include content match information and prevent further transmission of the one or more data packets based on the content match information. In contrast, Khan detects content match information in a first data packet containing the biometric information, and then determines whether to prevent transmission of different data packet(s) containing a message from the user. (Khan, paragraphs [0053], [0055], and [0061]). Claim 18 is distinguishable from Khan for at least these reasons.

Claims 19 and 21- 27 depend from Claim 18 and include features that further distinguish them from the prior art.

Independent Claim 28 has been amended to include the features of Claim 32 (now canceled), and recites:

An apparatus for controlling transmission of identifiable content over an information network, comprising:

- means for providing content match information for the content to a DED, wherein the DED is located in the information network along a transmission path of a plurality of data packets, wherein at least one data packet includes the content match information;
- means for receiving the at least one data packet in the DED;
- means for detecting the content match information in the at least one data packet in the DED, and
- means for issuing a prompt to a workstation based on the content match information when the content match information is detected in the at least one data packet; and
- means for transmitting a message among a plurality of DEDs along the transmission path to prevent transmitting more than one prompt for the same packet.

Khan does not teach or disclose "means for transmitting a message among a plurality of DEDs along the transmission path to prevent transmitting more than one prompt for the same packet." In contrast, the cited portion of Khan teaches using different biometrics. (Khan, paragraph [0061]). Claim 28 is distinguishable from Khan for at least these reasons.

KOEESTNER_BERTANI_LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0260
FAX (949) 251-0260

Claims 29-31 and 33-35 depend from Claim 28 and include features that further distinguish them from the prior art.

Claim 36 has been amended to include the features of Claim 37 (now canceled), and recites:

"An apparatus for controlling transmission of data packets in an information network, comprising:

a Regional Transaction Processor (RTP) operable to communicate with a Data Enabling Device (DED) and at least one workstation, wherein the DED is operable to detect content match information in at least one of the data packets, and further wherein the RTP comprises:

instructions operable to generate information to include in a prompt to be presented at the workstation, wherein the prompt is based on information in the at least one data packet, wherein the DED is operable to detect the content match information at a rate proportional to the rate at which the data packets are received."

Khan does not disclose or suggest detecting when the one or more data packets include content match information at a rate proportional to the rate at which the data packets are received. In contrast, the cited portions of Khan disclose using different types of biometrics, including the biometric on the envelope, and authenticating the sender's digital signature. (Khan, paragraphs [0060] and [0067]). Claim 36 is distinguishable from Khan for at least these reasons.

Claims 38-48 depend from Claim 36 and include features that further distinguish them from the prior art.

Claim 49 recites:

"An apparatus comprising:

a Central Storage and Backup System (CSBS) operable to communicate with a plurality of Regional Transaction Processors (RTPs) and to provide backup storage for the RTPs, wherein the RTPs are operable to communicate with a Data Enabling Device (DED) and at least one workstation, wherein the DED is operable to detect content match information in at least one of a plurality of data packets, and to prevent further transmission of the plurality of data packets based on the content match information in the at least one data packet, and further wherein the RTP comprises:

KOSTNER_BERTANI_LL P
18661 MACARTHUR BLVD
SUITE 400
IRVING, CA 92614
TEL: (949) 251-0250
FAX: (949) 251-0260

instructions operable to generate information to include in a prompt to be presented at the workstation, wherein the prompt is based on information in the plurality of data packets.”

Khan does not detect when the data packets include content match information and prevent further transmission of the plurality of data packets based on the information in the at least one data packet. In contrast, Khan detects content match information in a first data packet containing the biometric information, and then determines whether to prevent transmission of different data packet(s) containing a message from the user. (Khan, paragraphs [0053], [0055], and [0061]). Claim 49 is distinguishable from Khan for at least these reasons.

Claims 50-52 depend from Claim 49 and include features that further distinguish them from the prior art.

Independent Claim 53 recites:

“A computer program product comprising:
instructions to enable communication between a workstation, a Data Enabling Device (DED), and a Regional Transaction Processor (RTP), wherein the DED is operable to detect content match information in at least one data packet in a plurality of data packets and to prevent further transmission of the plurality of data packets based on the information in the at least one data packet, and further wherein the RTP is operable to generate information to include in a prompt to be presented at the workstation, wherein the prompt is based on information in the at least one data packet.”

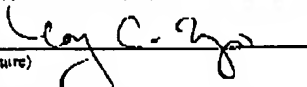
Khan does not detect when the data packets include content match information and prevent further transmission of the plurality of data packets based on the information in the at least one data packet. In contrast, Khan detects content match information in a first data packet containing the biometric information, and then determines whether to prevent transmission of different data packet(s) containing a message from the user. (Khan, paragraphs [0053], [0055], and [0061]). Claim 53 is distinguishable from Khan for at least these reasons.

KOESTNER BERTANI LLP
18661 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92613
TEL (949) 251-0150
FAX (949) 251-0260

CONCLUSION

Applicant believes the application, including all current claims 1-3, 5-19, 21-31, 33-35 and 38-53 are in form for allowance and a notice to that effect is solicited. In the event it would facilitate prosecution of this application, the Examiner is invited to telephone the undersigned at (949) 251-0250.

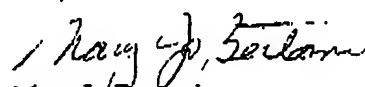
I hereby certify that this correspondence is being facsimile transmitted to the USPTO, Central Mailroom at (571) 273-8300 on the date shown below


(Signature)

Jay C. Ngo
(Printed Name of Person Signing Certificate)

November 28, 2005
(Date)

Respectfully submitted,


Mary Jo Bertani
Attorney for Applicant(s)
Reg. No. 42,321

KOESTNER BERTANI LLP
18662 MACARTHUR BLVD.
SUITE 400
IRVINE, CA 92612
TEL (949) 251-0250
FAX (949) 251-0250